arXiv:quant-ph/0502040v2 11 Apr 2005

Entangling Power of Permutations

Lieven Clarisse,[1,*] Sibasish Ghosh,[2,†] Simone Severini,[1,2,‡] and Anthony Sudbery[1,§]

[1] *Dept. of Mathematics, The University of York, Heslington, York YO10 5DD, U.K.*
[2] *Dept. of Computer Science, The University of York, Heslington, York YO10 5DD, U.K.*

The notion of *entangling power* of unitary matrices was introduced by Zanardi, Zalka and Faoro [PRA, 62, 030301]. We study the entangling power of permutations, given in terms of a combinatorial formula. We show that the permutation matrices with zero entangling power are, up to local unitaries, the identity and the swap. We construct the permutations with the minimum nonzero entangling power for every dimension. With the use of orthogonal latin squares, we construct the permutations with the maximum entangling power for every dimension. Moreover, we show that the value obtained is maximum over all unitaries of the same dimension, with possible exception for 36. Our result enables us to construct generic examples of 4-qudits maximally entangled states for all dimensions except for 2 and 6. We numerically classify, according to their entangling power, the permutation matrices of dimension 4 and 9, and we give some estimates for higher dimensions.

PACS numbers: 03.67.-a, 03.67.Mn

I. INTRODUCTION

The notion of entangling power of a quantum evolution was introduced by Zanardi, Zalka and Faoro [21] (see also [9, 19, 22]). Let $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ be Hilbert spaces where $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. The entangling power of a unitary $U \in \mathcal{U}(\mathcal{H}) \cong U(d^2)$ is the average amount of entanglement produced by U acting on a given (uncorrelated) distribution of product states. As the pure entanglement measure we use the linear entropy $S_L(\cdot)$ of the reduced density matrix. For $|\psi\rangle \in \mathcal{H}$, let [1]

$$S_L(|\psi\rangle) := \frac{d}{d-1}(1 - \operatorname{Tr}\rho^2), \quad \text{where} \quad \rho = \operatorname{Tr}_B |\psi\rangle\langle\psi|.$$

The *entangling power* of U is defined as [21]

$$\epsilon(U) := \int_{\langle\psi_1|\psi_1\rangle=1} \int_{\langle\psi_2|\psi_2\rangle=1} S_L(U|\psi_1\rangle|\psi_2\rangle) d\psi_1 d\psi_2, \tag{1}$$

where $d\psi_1$ and $d\psi_2$ are normalized probability measures on unit spheres. As the linear entropy is a concave function of the reduced density matrix, it is an entanglement monotone [17], and therefore a legitimate pure state entanglement measure.

Consider now the scenario where Alice and Bob share an unknown product state and want to use a unitary operator to create a state which is as highly entangled as possible. This means that Alice and Bob are looking for unitaries with the maximum entangling power. Zanardi [22] observed that there are permutation matrices with the maximum entangling power over all unitaries in $\mathcal{U}(\mathcal{H})$ when d is odd or $d = 4n$, but the case $d = 4n + 2$ was left open. In this paper we extend this result and study the entangling power $\epsilon(P)$ of a permutation matrix P.

The paper is organized as follows. In Section II we give a combinatorial expression for $\epsilon(P)$ (Theorem 2). In Section III we determine the non-entangling permutations (Theorem 3). In Section IV we construct permutations with the maximum entangling power over all unitaries in $\mathcal{U}(\mathcal{H})$ for every $d \neq 6$. Moreover, we construct permutations with the minimum entangling power for all d (Theorem 7). As a corollary, we give an upper bound to the number of permutations with different entangling power. In Section V, we give a complete numerical classification of permutation matrices of dimension 4 and 9 according to their entangling power. For higher dimensions, we report numerical estimates. Finally, in Section VI we draw conclusions and propose some open problems.

II. ENTANGLING POWER OF PERMUTATIONS

For our purposes we find it useful to rewrite Equation (1) in another more concrete form as described by Zanardi [22] (see Equation (3) in Lemma (1), below). The new expression for $\epsilon(U)$ is based on a correspondence between quantum operations on bipartite systems and certain quantum states which we are now going to recall.

Let $|\psi\rangle = \sum_{i,j} X_{ij}|ij\rangle$ be a state in $\mathcal{H}$ and let X be the corresponding operator on $\mathcal{H}$, so that $X_{ij} = d\langle i|X|j\rangle$. The singular values of X are equal to the Schmidt coefficients of $|\psi\rangle$. The state $|\psi\rangle$ can be written in terms of this operator as $|\psi\rangle = X \otimes I|\psi_+\rangle$, where $|\psi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$ is a maximally entangled state and I is the identity operator. This relation establishes a bijection between pure states in $\mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_B$ and operators X acting on $\mathcal{H}_A \cong \mathcal{H}_B$.

Now, following Cirac *et al.* [4], suppose $\mathcal{H}_A$ and $\mathcal{H}_B$ are themeselves bipartite: $\mathcal{H}_A = \mathcal{H}_1 \otimes \mathcal{H}_2$ and $\mathcal{H}_B = \mathcal{H}_3 \otimes \mathcal{H}_4$. We can repartition $\mathcal{H} \cong \mathcal{H}_A \otimes \mathcal{H}_B$ and regard it as the

*Electronic address: lc181@york.ac.uk
†Electronic address: sibasish@cs.york.ac.uk
‡Electronic address: ss54@york.ac.uk
§Electronic address: as2@york.ac.uk

tensor product of $\mathcal{H}_1 \otimes \mathcal{H}_3$ and $\mathcal{H}_2 \otimes \mathcal{H}_4$. Applying the above construction to an operator X_{13} yields a state

$$|X\rangle_{A|B} = |X\rangle_{12|34} := \frac{1}{N}(X_{13} \otimes I_{24})|\Psi_+\rangle_{13|24}, \qquad (2)$$

where

$$|\Psi_+\rangle_{13|24} = \frac{1}{d}\sum_{i,j=1}^{d} |ij\rangle_{13} \otimes |ij\rangle_{24},$$

and N is an appropriate normalization factor. This has an important physical interpretation: the operator X_{13}, acting on the Hilbert space $\mathcal{H}_{A1} \otimes \mathcal{H}_{B3}$, corresponds to a quantum operation. If this quantum operation is a tensor product of two quantum operations, one acting on the system 1 and another on the system 3, then $|X\rangle_{12|34}$ is a product state with respect to the systems A and B. In fact, $X_{13} \otimes I_{24}$ and $|X\rangle_{12|34}$ have the same Schmidt decomposition if X_{13} is a unitary operator [22]. It turns out that if both parties A and B share an entangled state $|X\rangle_{12|34}$ then the non-local quantum operation $X_{13} \otimes I_{24}$ can be implemented with certainty by making use of local operations and classical communication only (see Equation 6 of [4]). With this in mind, the entangling power of a unitary U is related to the entanglement of $|U\rangle$ as defined in Equation (2). We use the linear entropy as an entanglement measure. It might clarify matters to give the following two extremal examples:

- (Identity) If $U = I$ then the corresponding state is given by

  $$|I\rangle_{12|34} = \frac{1}{d}\sum_{i,j=1}^{d} |ii\rangle_{12} \otimes |jj\rangle_{34},$$

  which is separable with respect to the split $A|B = 12|34$. In this case we have $S_L(|I\rangle) = 0$.

- (Swap) If $U = S = \sum_{ij}^{d} |ij\rangle\langle ji|$ then the corresponding state is given by

  $$|S\rangle_{12|34} = |\Psi_+\rangle_{A|B} = \frac{1}{d}\sum_{i,j=1}^{d} |ij\rangle_{12} \otimes |ij\rangle_{34},$$

  which is a maximally entangled vector. In this case we have $S_L(|S\rangle) = 1$.

The swap corresponds to the parties interchanging their systems, and might therefore be regarded as the most non-local operation possible. Nevertheless, the swap operation is non-entangling (that is, it never creates entanglement). This discrepancy between *non-local* and *non-entangling* means that we cannot *just* use the entanglement of $|U\rangle$ as a measure for the entangling power of the matrix U. However with a small modification one can still express $\epsilon(U)$ in terms of the linear entropy, as is done in the following lemma.

Lemma 1 (Zanardi [22]) *The entangling power of a unitary $U \in \mathcal{U}(\mathcal{H})$ is given by*

$$\epsilon(U) = \frac{d}{d+1}[S_L(|U\rangle) + S_L(|US\rangle) - S_L(|S\rangle)], \qquad (3)$$

where $0 \leq \epsilon(U) \leq \frac{d}{d+1}$ [2].

A *permutation* of $[n] = \{1, 2, ..., n\}$ is a bijection from $[n]$ to itself. Every permutation p of $[n]$ induces an $n \times n$ matrix $P = (p_{ij})$, called a *permutation matrix*, such that $p_{ij} = 1$ if $p(i) = j$ and $p_{ij} = 0$ otherwise. Equivalently a permutation on $[n]$ induces a linear map of an n-dimensional Hilbert space which permutes a given basis of the space (a *permutation operator* on $\mathcal{H}$). If $n = d^2$ we can replace $[n]$ by $[d] \times [d]$ and write $p(i, j) = (k_{ij}, l_{ij})$; thus a permutation of $[d^2]$ is represented by a pair of $d \times d$ matrices $K = (k_{ij})$ and $L = (l_{ij})$. The corresponding permutation operator permutes the elements $|i\rangle|j\rangle$ of a product basis of $\mathcal{H}$:

$$P(|i\rangle|j\rangle) = |k_{ij}\rangle|l_{ij}\rangle.$$

Theorem 2 *Let $P = \sum_{ij} |k_{ij}l_{ij}\rangle\langle ij|$ be a permutation matrix in $\mathcal{U}(\mathcal{H})$. The entangling power of P is given by*

$$\epsilon(P) = \frac{d^4 + d^2 - Q_P - Q_{PS}}{d(d-1)(d+1)^2},$$

with

$$Q_P = \sum_{i,j,m,n=1}^{d} a_{ijm}a_{ijn}b_{imn}b_{jmn}, \qquad (4)$$

where

$$\begin{aligned} a_{ijm} &= \langle l_{im}|l_{jm}\rangle = a_{jim}, \\ b_{imn} &= \langle k_{im}|k_{in}\rangle = b_{inm}. \end{aligned}$$

The quantity Q_{PS} is the corresponding expression for the permutation PS.

Proof. ¿ From Lemma 1,

$$\epsilon(P) = \frac{d^4 + d^2 - d^4[\mathrm{Tr}\rho_{PS}^2 + \mathrm{Tr}\rho_P^2]}{d(d-1)(d+1)^2},$$

where ρ_P and ρ_{PS} are the reduced density matrices of the states $|P\rangle\langle P|$ and $|PS\rangle\langle PS|$, respectively. We can express $d^4\mathrm{Tr}\rho_P^2$ in terms of the matrices (k_{ij}) and (l_{ij}). Applying the formula in Equation 2, we find the state corresponding to P as

$$|P\rangle_{12|34} = \frac{1}{d}\sum_{i,m=1}^{d} |k_{im}i\rangle_{12} \otimes |l_{im}m\rangle_{34}.$$

This leads to

$$\rho_P = \mathrm{Tr}_B|P\rangle\langle P| = \frac{1}{d^2}\sum_{i,j,m=1}^{d} a_{ijm}|k_{im}i\rangle\langle k_{jm}j|.$$

By squaring and taking the trace, we obtain

$$d^4 \mathrm{Tr}\rho_P^2 = \sum_{i,j,m,n=1}^{d} a_{ijm}a_{ijn}b_{imn}b_{jmn}.$$

The same analysis applies to Q_{PS}. ■

QTPite The problem of classifying bipartite permutation operators according to their entangling power now reduces to finding what different values can be taken by $Q_P + Q_{PS}$. Observe that the coefficients a_{ijn} and b_{imn} (which are either 0 or 1), and the combination

$$r_{ijmn} = a_{ijm}a_{ijn}b_{imn}b_{jmn},$$

which occurs in (4), have the following interpretation:

- $a_{ijn} = 1$ if and only if (i,n) and (j,n), which are in the same column of the square $[d] \times [d]$, are taken by P to elements in the same column;
- $b_{imn} = 1$ if and only if (i,m) and (i,n), which are in the same row of the square, are taken by P to elements in the same row;
- $r_{ijmn} = 1$ if and only if $(i,m),(i,n),(j,m)$ and (j,n), which form a rectangle in $[d] \times [d]$, are taken by P to a rectangle with the same orientation.

We will denote the rectangle $(i,m),(i,n),(j,m),(j,n)$ (formed by the intersection of rows i and j and columns m and n) as R_{ijmn}. We note that if this rectangle is non-degenerate, that is $i \neq j$ and $m \neq n$, then it contributes either 0 or 4 to Q_P, since

$$r_{ijmn} = r_{jimn} = r_{ijnm} = r_{jinm} = 0 \text{ or } 1;$$

if $i = j$ or $m = n$ but not both, R_{ijmn} contributes 0 or 2; while if $i = j$ and $m = n$, then R_{ijmn} contributes 1.
QTPite
QTPite

III. NON-ENTANGLING PERMUTATIONS

QTPite Two permutation matrices $P, Q \in \mathcal{U}(\mathcal{H})$ are said to be *locally unitarily connected* (for short, *LU-connected*) if there are unitaries V acting on $\mathcal{H}_A$ and W on $\mathcal{H}_B$ such that $(V \otimes W)P = Q$. Then V and W are actually permutation operators. Note that if two permutations are LU-connected then they have the same entangling power. The set of non-entangling permutation matrices is denoted by E^0. The following result seems to be known to specialists (see, *e.g.*, [15]), but we provide a proof for completeness

Theorem 3 *Let $P \in \mathcal{U}(\mathcal{H})$ be a permutation matrix. Then $P \in E^0$ if and only if one of the following two conditions is satisfied:*

1. *P is LU-connected to I;*
2. *P is LU-connected to S.*

Proof. The permutation matrix P is non-entangling if $P(|\varphi\rangle|\chi\rangle)$ is a product state for all $|\varphi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B$. Consider two basis elements $|i\rangle|j_1\rangle$ and $|i\rangle|j_2\rangle$, and suppose

$$P(|i\rangle|j_1\rangle) = |i_1'\rangle|j_1'\rangle,$$
$$P(|i\rangle|j_2\rangle) = |i_2'\rangle|j_2'\rangle.$$

Then either $i_1' = i_2'$ or $j_1' = j_2'$, otherwise $P(|i\rangle(|j_1\rangle+|j_2\rangle))$ would be entangled. Suppose $i_1' = i_2' = i'$. Then for all j_3 we must have $P(|i\rangle|j_3\rangle) = |i'\rangle|j_3'\rangle$, for if not $P(|i\rangle|j_3\rangle) = |i''\rangle|j_1'\rangle$ and then $P(|i\rangle(|j_2\rangle + |j_3\rangle))$ is entangled. So there is a permutation p_B such that $P(|i\rangle|j\rangle) = |i'\rangle|p_B(j)\rangle$. Thus as a permutation of the square lattice $\{(i,j) : 1 \leq i,j \leq d\}$, P takes the row $(i,\cdot)$ to a row. Consider an element (i_2,j_1) in the same column as (i,j_1). The permutation p cannot take (i_2,j_1) to an element in the row $(i',\cdot)$, because that is already full. So p must take (i_2,j_1) to an element in the column $(\cdot,j_1')$. Thus p takes the column $(\cdot,j_1)$ to a column. It then follows that p takes every row to a row and every column to a column, that is $P((|i\rangle|j\rangle) = |p_A(i)\rangle|p_B(j)\rangle_2$ for some permutation p_A.

In the second case, $j_1' = j_2'$, the permutation p takes two elements in a row to elements in a column, and we can similarly show that it takes every row to a column and every column to a row, that is $P(|i\rangle|j\rangle) = |p_A(j)\rangle|p_B(i)\rangle$. ■

QTPite The probability of sampling a permutation matrix in E^0 over all permutations of $[d^2]$ goes to 0 as $d \to \infty$. In fact, by Theorem 3, the number of elements in E^0 is $2(d!)^2$, and therefore the probability is

$$\frac{2(d!)^2}{d^2!} \to 0 \text{ as } d \to \infty.$$

IV. ENTANGLING PERMUTATIONS

A. Maximum

QTPite In this section we construct and count the permutations with the maximum entangling power $d/(d+1)$ that can be attained by any unitary operator on $\mathcal{H}_A \otimes \mathcal{H}_B$. We will make use of latin squares. Recall that a *latin square* of *side* d is a $d \times d$ matrix with entries from the set $[d] = \{1,\ldots,d\}$ such that every row and column is a permutation of $\{1,\ldots,d\}$, and two $d \times d$ latin squares (k_{ij}) and (l_{ij}) are *orthogonal* if (k_{ij},l_{ij}) is a permutation of $[d] \times [d]$. Equivalently, two $d \times d$ latin squares (k_{ij}) and (l_{ij}) are orthogonal if the ordered pairs (k_{ij},l_{ij}) are distinct for all i and j. Euler believed that there are no orthogonal latin squares of side $4n+2$. Only in 1960 was it shown by Bose, Shrikhande and Parker that, except

for side 6, Euler's conjecture was false [3]. The study of latin squares is an important area of combinatorics with connections to design theory, projective geometries, graph theory, *etc.* [5, 6, 13]. Orthogonal latin squares have been recently applied in quantum information theory [8, 12, 18].

Theorem 4 *Let P be a permutation operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ defined by $P(|i\rangle|j\rangle) = |k_{ij}\rangle|l_{ij}\rangle$. Then the entangling power of P equals the maximum value $\epsilon(P) = d/(d+1)$ over $\mathcal{U}(\mathcal{H})$ if and only if the matrices (k_{ij}) and (l_{ij}) are orthogonal latin squares.*

Proof. By Theorem 2, the entangling power of P is maximised when $Q_P + Q_{PS}$ is minimised. Now Q_P is equal to the number of rectangles in $[d] \times [d]$ which are taken to rectangles by P, with the horizontal lines remaining horizontal and the vertical lines remaining vertical. This is at least d^2, since every rectangle consisting of a single point must be taken to a rectangle. It is precisely d^2 if and only if no nonzero horizontal line is taken to a horizontal line and no nonzero vertical line is taken to a vertical line, i.e. if

$$k_{im} \neq k_{in} \quad \text{whenever} \quad m \neq n$$

and

$$l_{im} \neq l_{jm} \quad \text{whenever} \quad i \neq j.$$

On the other hand, Q_{PS} is equal to the number of rectangles in $[d] \times [d]$ which are taken to rectangles by P, but with the horizontal lines becoming vertical and the vertical lines becoming horizontal. This will be precisely d^2 if and only if no nonzero vertical line is taken to a horizontal line and vice versa, that is if and only if

$$k_{im} \neq k_{jm} \quad \text{whenever} \quad i \neq j$$

and

$$l_{im} \neq l_{in} \quad \text{whenever} \quad m \neq n.$$

Together, these are the conditions for the matrices (k_{ij}) and (l_{ij}) to be latin squares. Since (k_{ij}, l_{ij}) form a permutation of (i, j), the two latin squares are orthogonal. ■

Corollary *For every $d \neq 2, 6$ there is a permutation matrix $P \in \mathcal{U}(\mathcal{H})$ such that $\epsilon(P)$ is maximum over $\mathcal{U}(\mathcal{H})$.*

Proof. It follows from Theorem 4 together with the fact that there are two orthogonal latin squares for every $d \neq 2, 6$ (see, *e.g.*, [6]). ■

As an example of a permutation matrix satisfying Theorem 4, consider

$$R = \left[\begin{array}{ccc|ccc|ccc} 1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1&0\\ \hline 0&0&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0&0 \end{array}\right].$$

For the permutation matrix R we have $\epsilon(R) = \frac{3}{4}$ which is the maximum over all unitaries in $\mathcal{U}(\mathcal{H}) = (\mathcal{H}_A \otimes \mathcal{H}_B)$ where $\dim \mathcal{H}_A = \dim \mathcal{H}_B = 3$.

By looking at $d^2 \times d^2$ permutation matrices as made up of d^2 blocks, we can state an alternative version of Theorem 4.

Theorem 5 *Let $P \in \mathcal{U}(\mathcal{H})$ be a permutation matrix. Then $\epsilon(P)$ is maximum over $\mathcal{U}(\mathcal{H})$ if and only if P satisfies the following conditions:*

1. *Every block contains one and only one nonzero element;*
2. *All blocks are different;*
3. *Nonzero elements in the same block-row are in different sub-columns;*
4. *Nonzero elements in the same block-column are in different sub-rows.*

Proof. By Theorem 2, the quantity Q_P is maximum if and only if $a_{ijm} = b_{imn} = 1$ for all $1 \leq i, j, n, m \leq d$. In this case $Q_P = d^4$ (for example, when $P = I$). On the other hand Q_P is minimum if and only if $a_{ijn} = \delta_{ij}$ and $b_{imn} = \delta_{mn}$, and in this case the sum reduces to

$$Q_P = \textstyle\sum_{i,n=1}^{d} a_{iin} b_{inn} = d^2 \quad \text{(for example, when } P = S\text{)}.$$

To obtain the maximum entangling power we need to find the permutation matrix that minimizes $Q_P + Q_{PS}$. We have seen that the maximum entangling power is $d/(d+1)$, and in [22] is shown that this value can be obtained if and only if

$$S_L(|U\rangle) = S_L(|US\rangle) = S_L(|S\rangle)$$

or, equivalently,

$$Q_P = Q_{PS} = Q_S = d^2.$$

It is then easy to observe that the conditions 1 and 2 express the minimality of Q_P and the conditions 3 and 4 express the minimality of Q_{PS}. ■

Theorem 5 implies that in a $d^2 \times d^2$ permutation matrix P attaining the maximum value $d/(d+1)$, every block

contains one and only one nonzero entry (as in the above permutation matrix R). It is then possible to represent P by a $d \times d$ array $\widetilde{P} = (\widetilde{p}_{ij})$. The cell $\widetilde{p}_{ij}$ specifies the coordinates of the nonzero entry in the ij-th block of P. For the above permutation matrix R, we have

$$\widetilde{R} = \begin{array}{|ccc|}\hline 11 & 23 & 32 \\ 22 & 31 & 13 \\ 33 & 12 & 21 \\ \hline \end{array}\,.$$

Note that the ij-th cell of $\widetilde{R}$ is of the form (k_{ij}, l_{ij}) where $K = (k_{ij})$ and $L = (l_{ij})$ are the orthogonal latin squares

$$K = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline \end{array} \text{ and } L = \begin{array}{|ccc|}\hline 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \\ \hline \end{array}\,.$$

It follows from Theorem 5 that a permutation matrix P has maximal entangling power if and only if $\widetilde{P}$ is obtained by *superimposing* two orthogonal latin squares.

Direct calculations give the following result.

Theorem 6 *The following statements are true:*

1. *For $d = 2$ the matrix $P = CNOT$ attains the value $\epsilon(P) = \frac{4}{9}$ which is maximum over all unitaries in $\mathcal{U}(\mathcal{H})$.*

2. *For $d = 6$ the value $\epsilon(P) = \frac{628}{735}$ is maximum over all permutations $P \in \mathcal{U}(\mathcal{H})$ and the maximizing P is associated to*

$$\widetilde{P} = \begin{array}{|cccccc|}\hline 11 & 22 & 33 & 44 & 55 & 66 \\ 23 & 14 & 45 & 36 & 61 & 52 \\ 32 & 41 & 64 & 53 & 16 & 25 \\ 46 & 35 & 51 & 62 & 24 & 13 \\ 54 & 63 & 26 & 15 & 42 & 31 \\ 65 & 56 & 12 & 21 & 33 & 44 \\ \hline \end{array}\,. \qquad (5)$$

Proof. *Part 1.* It has been shown by Rezakhani [15] that for $d = 2$, the entangling power of any unitary $U \in U(4)$ is given by

$$\epsilon(U) = \frac{1}{3} - \frac{1}{9} \times \{\cos(4c_1)\cos(4c_2) + \cos(4c_1)\cos(4c_3) + \cos(4c_2)\cos(4c_3))\}, \qquad (6)$$

where $c_1, c_2, c_3 \in \mathbb{R}$ and $|c_3| \leq c_2 \leq c_1 \leq \pi/4$. It is easy to show that $\epsilon(U)$ takes its maximum value $4/9$ when either $c_1 = c_2 = \pi/4, c_3 = 0$ or $c_1 = \pi/4, c_2 = c_3 = 0$. Then, every permutation matrix which is LU-connected to any of the four matrices attains this maximum value (see Table I, given in Section V):

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},\ S \cdot CNOT,$$

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad S \cdot M.$$

Part 2. The permutation associated to $\widetilde{P}$ arises from the latin squares

$$\begin{array}{|cccccc|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 4 & 6 & 5 & 1 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 1 & 2 & 3 & 4 \\ \hline \end{array}$$

and

$$\begin{array}{|cccccc|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 6 & 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ 5 & 6 & 2 & 1 & 3 & 4 \\ \hline \end{array}\,,$$

which are *'as close to being orthogonal as possible'* [11]. For P, we have that $Q_P = 40$ and $Q_{PS} = 36$. Since there do not exist two orthogonal latin squares of side 6, these are the smallest values obtainable, as it is explained by the following argument. The array

$$\widehat{P} = \begin{array}{|cccccc|}\hline 11 & 22 & \mathbf{33} & \mathbf{44} & 55 & 66 \\ 24 & 13 & 46 & 35 & 62 & 51 \\ 56 & 65 & 12 & 21 & 43 & 34 \\ 63 & 54 & 25 & 16 & 31 & 42 \\ 45 & 36 & 61 & 52 & 14 & 23 \\ 32 & 41 & \mathbf{53} & \mathbf{64} & 26 & 15 \\ \hline \end{array}$$

represents the action of P on the set $[6] \times [6]$. The ij-th cell of $\widehat{P}$ is kl if in P the contribution of the term $|kl\rangle\langle ij|$ is nonzero (for example, the 22-th cell of $\widehat{P}$ is 13 because $|13\rangle\langle 22|$ is nonzero in P). We have printed in boldface the symbols that occur twice in a row or in a column. Observe that, given any permutation matrix $P \in U(36)$, since every element of the set $[6]\times[6]$ has to occur exactly once in $\widehat{P}$, it is never possible to have only one pair of equal symbols in the same column, without this being the case for also another column. Hence, the minimum

value attainable by Q_P would be 2 steps ahead of 36, that is 40. ■

We have established a bijection between pairs of orthogonal latin squares of side d and $d^2 \times d^2$ permutations with maximal entangling power. The number of pairs of orthogonal latin squares of side d is known only for small d (see A072377, [16]). It is 36 for $d = 3$ and 3456 for $d = 4$. Note that these values apply to unordered pairs of orthogonal latin squares. This means that the number of $d^2 \times d^2$ permutations with the maximum entangling power is twice the number of pairs of orthogonal latin squares of side d. General methods for constructing pairs of orthogonal latin squares are presented in [6, 7, 14].

For a unitary U that reaches the upper bound $\epsilon(U) = d/(d+1)$, we have $S_L(|U\rangle) = S_L(|US\rangle) = 1$. In other words, $|U\rangle$ is maximally entangled with respect to the bipartite splits 12|34 and 23|14. It turns out that this is also maximally entangled with respect to the split 13|24. The easiest way to see this is by looking at Equation 2 defining $|U\rangle$. The state $|U\rangle_{13|24}$ is obtained by two parties $A = 13$ and $B = 24$ sharing a maximally entangled state, by applying the unitary U on Alice's system. Since this is a local reversible transformation, the entanglement is preserved, hence the state $|U\rangle_{13|24}$ is maximally entangled. Thus a unitary U is maximally entangling if and only $|U\rangle$ is maximally entangled with respect to the three possible bipartite splits [20]. Note that $|U\rangle$ is also maximally entangled in all the four splits 1|234, 2|134, 3|124 and 4|123. Then $|U\rangle$ is indeed a maximally entangled state. The construction of maximally entangling unitaries thus provides us with a canonical way of constructing such maximally entangled 4-qudits for all dimensions except $d = 2$ and $d = 6$. It has been known for some time that this is not possible for $d = 2$, *i.e.* 4-qubits (see [10]), leaving only the case $d = 6$ open.

B. Minimum

In this section we construct the permutations with the minimum nonzero entangling power that can be attained by permutation operators on $\mathcal{H}_A \otimes \mathcal{H}_B$. Two permutation matrices $P, Q \in \mathcal{U}(\mathcal{H})$ are said to be in the same *entangling class* if $\epsilon(P) = \epsilon(Q)$.

Theorem 7 *Let $P \in \mathcal{U}(\mathcal{H})$ be a permutation matrix. Then $\epsilon(P)$ is nonzero but minimum over all permutations in $\mathcal{U}(\mathcal{H})$ if*

$$\widehat{P} = \begin{array}{|cccc|} \hline 11 & 12 & \cdots \cdots & 1d \\ 21 & 22 & \cdots \cdots & 2d \\ \vdots & \vdots & & \vdots \\ (d-1)1 & (d-1)2 & \cdots \cdots & (d-1)d \\ d1 & d2 & \cdots dd & d(d-1) \\ \hline \end{array} .$$

In such a case

$$\epsilon(P) = \frac{8(d-1)}{d(d+1)^2}. \tag{7}$$

Proof. Since P is the permutation matrix *closest* to I, it is clear that $\epsilon(P)$ is miminum. To find its value, we compare Q_P with Q_I where I denotes the identity permutation. The rectangles R_{ijmn} which contribute to Q_I but not to Q_P are those containing $(d-1, d)$ or (d, d) or both, except for the degenerate rectangles contained in the bottom line of the square (i.e. those with $i = j = d$). There are $(d-1)(d-2)$ non-degenerate rectangles containing $(d-1, d)$ but not $(d, d-1)$, each contributing 4 to Q_I, and $d-1$ degenerate vertical rectangles, with two equal vertices at $(d, d-1)$ and two equal vertices at $(i, d-1)$ where $i \neq d$. Each of these contributes 2 to Q_I, so the total contribution from rectangles containing $(d, d-1)$ but not (d, d) is $4(d-1)(d-2) + 2(d-1)$. There is an equal contribution from rectangles containing (d, d) but not $(d, d-1)$. Finally, there are $d-1$ non-degenerate rectangles containing both $(d, d-1)$ and (d, d), each contributing 4 to Q_I. The total contribution to Q_I which is not included in Q_P is $8(d-1)^2$. Since $Q_I = d^4$, we have

$$Q_P = d^4 - 8(d-1)^2.$$

On the other hand, $Q_{PS} = d^2$ since no nonzero horizontal line is taken to a vertical line by P. Hence, by Theorem 2, $\epsilon(P)$ is given by (7). ■

Corollary *An upper bound to the number of different entangling classes of permutations is given by*

$$B = 2 + \frac{1}{2}(d^4 - d^2 - 8(d-1)^2). \tag{8}$$

Proof. We can write $Q_P = \sum_{i,j,m,n=1}^{d} r_{ijmn}$. If $i \neq j$ and $m \neq n$, the contribution of the rectangle R_{ijmn} is 0 or 4, which is even. If either $i = j$ or $m = n$, the contribution of R_{ijmn} is 0 or 2, which is again even. If $i = j$ and $m = n$, the contribution of R_{ijmn} is 1, and in total we have d^2 such terms. It follows that Q_P is even if and only if d is even. The same analysis applies to Q_{PS}. Then $Q_P + Q_{PS}$ is even for all d.

Now we have seen that the zero entangling power corresponds to $Q = d^4 + d^2$, and the maximum to $Q = 2d^2$, so that $\frac{1}{2}(d^4 - d^2 + 2)$ is an upper bound to the number of classes, where the coefficient $1/2$ comes from the fact that two consecutives values of Q_P (Q_{PS}) differ by a multiple of 2. We can tighten this bound and obtain the value $(B-2)$ by making use of the fact from Theorem 7 that the value of $Q_P + Q_{PS}$ is $d^4 - 8(d-1)^2 + d^2$ when $\epsilon(P)$ is nonzero but minimum. The first term 2 on the RHS of Equation 8 occurs because of the two classes corresponding to zero and the maximum entangling power. ■

V. NUMERICAL RESULTS

In this section we report some numerical results. We are interested in counting the number of different entangling classes for different dimensions. We are also interested in the average entangling power over all permutations of a given dimension. The results are given in the following tables:

Entangling Power $\epsilon(P)$	Number of elements in entangling class
0	8
4/9	16

TABLE I: Classes of permutations with different entangling power and the number of elements in each class for $d = 2$.

Entangling Power $\epsilon(P)$	Number of elements in entangling class
0	72
1/3	2592
3/8	864
5/12	1296
182/375	10368
23/48	20736
1/2	27432
25/48	36288
13/24	44064
9/16	101376
7/12	44712
29/48	46656
5/8	22464
2/3	3888
3/4	72

TABLE II: Classes of permutations with different entangling power and the number of elements in each class for $d = 3$.

Dimension d	Number of classes	Average entangling power
2	2	$\frac{8}{27} \approx 0.29$
3	15	$\frac{31}{56} \approx 0.55$
4	≥ 65	0.67 ± 0.01
5	≥ 190	0.74 ± 0.01

TABLE III: Number of classes of permutations with different entangling power and the average entangling power as a function of the dimension d.

VI. CONCLUSION AND OPEN PROBLEMS

In this paper we have studied the entangling power of permutations. We have shown that the permutation matrices with zero entangling power are, up to local unitaries, the identity and the swap. For all dimensions, we have constructed the permutations with (nonzero) minimum entangling power. With the use of orthogonal latin squares, we have constructed the permutations with the maximum entangling power for every dimension. Moreover, we have shown that this value is maximum over all unitaries of the same dimension, with a possible exception for 36. Our result enabled us to construct generic examples of 4-qudits maximally entangled states for all dimensions except for 2 and 6. We have reported numerical results about a complete classification of permutation matrices of dimension 4 and 9 according to their entangling power.

We conclude with a list of open problems:

- Describe a general classification of the permutation matrices according to their entangling power.
- Give a formula for the average entangling power over all permutation matrices of a given dimension.
- For $d = 6$, does there exist $U \in \mathcal{U}(\mathcal{H})$ such that $\epsilon(U) > \frac{628}{735}$?
- The formula in Equation (3) only works for the linear entropy. It would be desirable to have a similar simple formula of the entangling power of a unitary in terms of the von Neumann entropy.
- Study the entangling power of permutation matrices in relation to multipartite systems. In this context, it is conceivable that the permutation matrices with maximum entangling power are related to sets of mutually orthogonal latin squares.

Acknowledgements. We would like to thank S. L. Braunstein for helpful comments, and Ch. Zalka for pointing out the connection between maximally entangling unitaries and 4-qudit states that are maximally entangled with respect to all bipartite splits. LC is supported by a WW Smith Scholarship. SG and SS are supported by EPSRC grants GR/87406 and GR/S56252, respectively.

[1] In refs. [21] and [22], $S_L(|\psi\rangle)$ is taken as $S_L(|\psi\rangle) = 1-\mathrm{Tr}\rho^2$, where $\rho = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. In order to have $S_L(|\psi\rangle) \in [0,1]$, we have taken $S_L(|\psi\rangle) = \frac{d}{d-1}(1-\mathrm{Tr}\rho^2)$.

[2] In ref. [21], the coefficient in front of the term $[S_L(|U\rangle) + S_L(|US\rangle) - S_L(|S\rangle)]$ is $\left(\frac{d-1}{d+1}\right)\frac{1}{S_L(|S\rangle)}$, which in our case is $\frac{d}{d+1}$, as we used a modified definition of $S_L(|\psi\rangle)$.

[3] R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math* **12** (1960), 189–203.

[4] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Entangling Operations and Their Implementation Using a Small Amount of Entanglement, *Phys. Rev. Lett.* **86**, 544 (2001).

[5] C. J. Colbourn and J. H. Dinitz (eds.), The CRC handbook of combinatorial designs, CRC Press Series on Discrete Mathematics and its Applications, *CRC Press, Boca Raton, FL* (1996).

[6] J. Dénes and A. D. Keedwell (eds.), Latin Squares: New Developments in the Theory and Applications, *North-Holland, Amsterdam* (1991).

[7] M.-N. Gras, Une construction explicite de carrés latin orthogonaux d'ordre n pair, $n \geq 10$, *J. Alg.* **219**, 369 (1999).

[8] A.Hayashi, M.Horibe and T.Hashimoto, The king's problem with mutually unbiased bases and orthogonal Latin squares, quant-ph/0502092.

[9] A. Hamma and P. Zanardi, Quantum entangling power of adiabatically connected Hamiltonians, *Phys. Rev. A* **69**, 062319 (2004).

[10] A. Higuchi and A. Sudbery, How entangled can two couples get? *Phys. Lett. A* **273**, 213–217 (2000).

[11] R. Hill, A First Course in Coding Theory, *Clarendon Press, Oxford* (1986).

[12] A. Klappenecker and M. Rötteler, Unitary error bases: constructions, equivalence, and applications, Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003), 139–149, Lecture Notes in Comput. Sci., 2643, *Springer, Berlin* (2003).

[13] C. F. Laywine and G. L. Mullen, Discrete mathematics using Latin squares, Wiley-Interscience Series in Discrete Mathematics and Optimization, A Wiley-Interscience Publication. *John Wiley & Sons, Inc., New York* (1998).

[14] Z. Lie, A short disproof of Euler's conjecture concerning orthogonal Latin squares, With editorial comment by A. D. Keedwell, *Ars Combin.* **14** (1982), 47–55.

[15] A. T. Rezakhani, Characterization of two-qubit perfect entanglers, *Phys. Rev. A* **70**, 052313 (2004).

[16] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at: http://www.research.att.com/~njas/sequences/.

[17] G. Vidal, Entanglement monotones, *J. Mod. Opt.* **47**, 355 (2000).

[18] K. G. H. Vollbrecht and R. F. Werner, Why two qubits are special, *J. Math. Phys.* **41** (2000), 6772–6782.

[19] X. Wang and P. Zanardi, Quantum entanglement of unitary operators on bi-partite systems, *Phys. Rev. A* **66**, 044303 (2002).

[20] Ch. Zalka, *Private communication*.

[21] P. Zanardi, Ch. Zalka, and L. Faoro, Entangling power of quantum evolutions, *Phys. Rev. A* **62**, 030301 (2000).

[22] P. Zanardi, Entanglement of quantum evolutions, *Phys. Rev. A* **63**, 040304 (2001).